O. Forster: Seminar zur Zahlentheorie

SoSe 2023 am Math. Inst. der LMU
Mittwochs 14-16 Uhr, Raum A027

Bezeichnungen:

$\mathbb{N}_0 := \{n \in \mathbb{Z} : n \geqslant 0\}$,

$\mathbb{N}_1 := \{n \in \mathbb{Z} : n \geqslant 1\}$,

$\#X =$ Anzahl der Elemente einer endlichen Menge X.

A. Zahlentheoretische Funktionen und Dirichlet-Reihen

Eine zahlentheoretische (oder arithmetische) Funktion ist eine Abbildung

$$a : \mathbb{N}_1 \longrightarrow \mathbb{C},$$

d.h. eine Folge $(a(n))_{n\geqslant 1}$ von komplexen Zahlen. Oft liegen die Werte schon in $\mathbb{N}_1$, $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$. Einige Beispiele:

a) $\mathbb{1} : \mathbb{N}_1 \longrightarrow \mathbb{N}_1, \quad \mathbb{1}(n) = 1$ für alle $n \in \mathbb{N}_1$.

b) $\delta_1 : \mathbb{N}_1 \to \mathbb{N}_1, \quad \delta_1(n) = \delta_{1n} = \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{für } n \neq 1. \end{cases}$

c) Die identische Abbildung

$$\iota : \mathbb{N}_1 \longrightarrow \mathbb{N}_1, \quad \iota(n) = n \quad \text{für alle } n \in \mathbb{N}_1.$$

d) Teiler-Anzahlfunktion

$$\tau(n) = \text{Anzahl der (positiven) Teiler von } n \text{ (einschließlich 1 und } n),$$

z.B. $\tau(1) = 1,\ \tau(2) = 2,\ \tau(4) = 3,\ \tau(36) = 9,\ \tau(37) = 2, \ldots$.

e) Eulersche Phi-Funktion,

$$\varphi : \mathbb{N}_1 \to \mathbb{N}_1, \quad \varphi(n) := \#(\mathbb{Z}/n)^*.$$

Es ist also $\varphi(n) = \#\{k \in \{1, 2, \ldots, n\} : \gcd(k, n) = 1\}$.

f) Charakteristische Funktion der Menge der Primzahlen

$$\mathbb{1}_{\mathbb{P}} : \mathbb{N}_1 \longrightarrow \mathbb{N}_1, \quad \mathbb{1}_{\mathbb{P}}(n) = \begin{cases} 1, & \text{falls } n \text{ Primzahl}, \\ 0 & \text{sonst.} \end{cases}.$$

g) $\log : \mathbb{N}_1 \longrightarrow \mathbb{R}, \quad n \mapsto \log(n)$.

h) Von Mangoldtsche Funktion

$$\Lambda : \mathbb{N}_1 \longrightarrow \mathbb{R}, \quad \Lambda(n) = \begin{cases} \log p, & \text{falls } n = p^k, \ (p \text{ prim}, k \geqslant 1), \\ 0 & \text{sonst.} \end{cases}$$

i) $\Lambda_1 : \mathbb{N}_1 \longrightarrow \mathbb{Q}, \quad \Lambda_1(n) = \begin{cases} \frac{1}{k}, & \text{falls } n = p^k, \ (p \text{ prim}, k \geqslant 1), \\ 0 & \text{sonst.} \end{cases}$

Es gilt $\Lambda_1(n) \log(n) = \Lambda(n)$ für alle $n \in \mathbb{N}_1$.

j) Beispiel einer Funktion, die auch nicht-reelle Werte annimmt.

$$c : \mathbb{N}_1 \longrightarrow \mathbb{C}, \quad c(n) := \begin{cases} 0, & \text{falls } n \equiv 0 \bmod 5, \\ 1, & \text{falls } n \equiv 1 \bmod 5, \\ i, & \text{falls } n \equiv 2 \bmod 5, \\ -i, & \text{falls } n \equiv 3 \bmod 5, \\ -1, & \text{falls } n \equiv 4 \bmod 5. \end{cases}$$

Definition. Eine arithmetische Funktion $f : \mathbb{N}_1 \to \mathbb{C}$ heißt *multiplikativ*, falls $f(1) = 1$ und

$$f(nm) = f(n)f(m) \quad \text{für alle } n, m \in \mathbb{N}_1 \text{ mit } \gcd(n, m) = 1.$$

Die Funktion f heißt *vollkommen multiplikativ*, falls die Bedingung $f(nm) = f(n)f(m)$ ohne Einschränkung gilt.

Ist f multiplikativ, so braucht man die Werte von f nur für die Primzahlpotenzen zu kennen, denn aus $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ folgt

$$f(n) = f(p_1^{k_1}) \cdot \ldots \cdot f(p_r^{k_r}).$$

Die Teiler-Anzahlfunktion τ und die Eulersche Phi-Funktion sind multiplikativ; die Funktionen $\mathbb{1}$, δ_1, ι und die Funktion c aus Beispiel j) sind sogar vollkommen multiplikativ.

Beispiele. i) Die Teiler einer Primzahlpotenz p^k sind $1, p, p^2, \ldots, p^k$, also $\tau(p^k) = k + 1$. Es folgt

$$\tau(p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}) = \prod_{\nu=1}^{r} (k_\nu + 1).$$

Z.B. ist $36 = 2^2 \cdot 3^2$, also $\tau(36) = (2 + 1)(2 + 1) = 9$.

ii) Für die Eulersche Phi-Funktion gilt

$$\varphi(p^k) = p^k - p^{k-1} = p^k\Big(1 - \frac{1}{p_k}\Big),$$

denn genau die p^{k-1} Vielfachen von p sind unter den Zahlen $1, 2, \ldots, p^k$ nicht teilerfremd zu p^k. Es folgt

$$\varphi(p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}) = \prod_{\nu=1}^{r} p_\nu^{k_\nu}\Big(1 - \frac{1}{p_\nu^{k_\nu}}\Big).$$

Die lässt sich vereinfachen zu

$$\varphi(n) = n \prod_{p|n}\Big(1 - \frac{1}{p}\Big),$$

wobei das Produkt über alle Primteiler p von n zu bilden ist.

Summatorische Funktion. Ist $f : \mathbb{N}_1 \to \mathbb{C}$ eine arithmetische Funktion, so versteht man unter der summatorischen Funktion von f die Funktion $F : \mathbb{N}_1 \to \mathbb{C}$ mit

$$F(n) := \sum_{k|n} f(k),$$

wobei über alle Teiler $k \mid n$ zu summieren ist.

Beispiele. i) Die Teiler-Anzahlfunktion τ lässt sich schreiben als

$$\tau(n) = \sum_{k|n} 1 = \sum_{k|n} \mathbb{1}(k),$$

Die Funktion τ ist also summatorische Funktion der Funktion $\mathbb{1}$.

ii) Summatorische Funktion der Eulerschen Phi-Funktion. Es gilt

$$\sum_{k|n} \varphi(k) = n,$$

die summatorische Funktion von φ ist also die Funktion ι aus Beispiel c).

Beweis. Die Menge $M_n = \{1, 2, \ldots, n\}$ ist die disjunkte Vereinigung der Mengen

$$A_k(n) := \{m \in M_n : \gcd(n, m) = k\}.$$

Da $\gcd(n, m) = k$ genau dann, wenn $k \mid n$, $k \mid m$ und $\gcd(n/k, m/k) = 1$, ist $\#A_k(n) = \#A_1(n/k) = \varphi(n/k)$. Es folgt

$$n = \#M_n = \sum_{k|n} \#A_k(n) = \sum_{k|n} \varphi(n/k) = \sum_{k|n} \varphi(k),$$

denn durchläuft k alle Teiler von n, so durchläuft auch n/k alle Teiler von n.

iii) Für die Mangoldtsche Funktion $\Lambda : \mathbb{N}_1 \to \mathbb{R}$ (Beispiel h) gilt

$$\sum_{d|n} \Lambda(d) = n.$$

Es gilt der Satz:

Satz. *Sei $f : \mathbb{N}_1 \to \mathbb{C}$ eine multiplikative arithmetische Funktion. Dann ist auch die summatorische Funktion F von f multiplikativ.*

Beispielsweise ist die Teiler-Funktion τ die summatorische Funktion der Funktion $\mathbb{1}$. Da letztere trivialerweise multiplikativ ist, gibt dies einen neuen Beweis der Multiplikativität von τ.

Zugeordnete Dirichlet-Reihen. Jeder arithmetischen Funktion $a : \mathbb{N}_1 \to \mathbb{C}$ kann man eine sog. Dirichlet-Reihe

$$f(s) := \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

zuordnen. Dies ist zunächst nur eine formale Reihe. Aber für alle bisher behandelten Beispiele gibt es ein $s_0 \in \mathbb{R}$, so dass die Reihe für alle $s > s_0$ konvergiert.

Beispiele von Dirichlet-Reihen

i) Für die arithmetische Funktion $\mathbb{1}$ (Beispiel a) erhält man die Zetafuntion

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Sie konvergiert für alle $s > 1$.

ii) Die charakteristische Funktion der Menge der Primzahlen (Beispiel f) ergibt die sog. *Primzeta-Funktion*

$$\mathcal{P}(s) = \sum_{p} \frac{1}{p^s}$$

Dabei wird über alle Primzahlen summiert. Dies Reihe konvergiert ebenfalls für alle $s > 1$.

Die Koeffizienten $a(n)$ einer Diruchlet-Reihe $f(s) = \sum_{n \geqslant 1} a(n)/n^s$ sind durch die Funktion $f(s)$ eindeutig bestimmt. Dies folgt aus dem Identitätssatz.

Satz (Identitätssatz für Dirichlet-Reihen). *Sei* $f(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ *eine Dirichlet-Reihe, die für wenigstens ein* $s \in \mathbb{R}$ *absolut konvergiert. Es gebe eine Folge* $(s_\nu)_{\nu \geqslant 1}$ *mit* $\lim_{\nu \to \infty} s_\nu = \infty$*, so dass*

$$f(s_\nu) = 0 \quad \textit{für alle } \nu.$$

Dann gilt $a(n) = 0$ *für alle* $n \in \mathbb{N}_1$.

Dirichlet-Faltung und Produkt von Dirichlet-Reihen

Sind $a, b : \mathbb{N}_1 \to \mathbb{C}$ zwei arithmetische Funktionen, so definiert man ihre Dirichlet-Faltung $c = a * b : \mathbb{N}_1 \to \mathbb{C}$ durch

$$(a * b)(n) := \sum_{k|n} a(k)b(n/k) = \sum_{k|n} a(n/k)b(k).$$

Dies lässt sich in symmetrischer Form auch so schreiben:

$$(a * b)(n) = \sum_{k\ell = n} a(k)b(\ell).$$

Dabei wird über alle Paare $k, \ell \in \mathbb{N}_1$ mit $k \cdot \ell = n$ summiert.

Speziell für $b = \mathbb{1}$ (Funktion aus Beispiel a) ergibt sich

$$(a * \mathbb{1})(n) = \sum_{k\ell=n} a(k)\mathbb{1}(\ell) = \sum_{k|n} a(k).$$

Die Dirichlet-Faltung von a mit der Funktion $\mathbb{1}$ erzeugt also die summatorische Funktion von a.

Der Dirichlet-Faltung zweier arithmetischer Funktionen entspricht das Produkt der zugeordneten Dirichlet-Reihen.

$$\Big(\sum_{k=1}^{\infty} \frac{a(k)}{k^s}\Big)\Big(\sum_{\ell=1}^{\infty} \frac{b(\ell)}{\ell^s}\Big) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s}$$

mit $\quad c(n) = (a * b)(n) := \sum_{k\ell=n} a(k)b(\ell) = \sum_{k|n} a(k)b(n/k).$

Über das Konvergenzverhalten von Dirichlet-Reihen gibt folgender Satz Auskunft:

Satz. *Sei* $f(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ *eine Dirichlet-Reihe. Es existiere ein* $s_0 \in \mathbb{R}_+$*, so dass*

$$A(x) := \sum_{n\leqslant x} a(n) = O(x^{s_0}) \quad \textit{für } x \to \infty.$$

Dann konvergiert die Reihe $f(s)$ *für alle* $s > s_0$*. Die Funktion* $f(s)$ *ist dort sogar differenzierbar mit*

$$f'(s) = -\sum_{n=1}^{\infty} \frac{\log(n)a(n)}{n^s}.$$

Zum Beweis benutzt man folgenden Satz

Satz (Abelsche partielle Summation). *Sei* $a : \mathbb{N}_1 \to \mathbb{C}$ *eine zahlentheoretische Funktion und*

$$A(x) := \sum_{n\leqslant x} a(n).$$

Weiter sei $f : [1, \infty[\to \mathbb{R}$ *eine stetig differenzierbare Funktion. Dann gilt für alle* $x \geqslant 1$

$$\sum_{n\leqslant x} a(n)f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt.$$

Logarithmus der Zetafunktion

$$\log\zeta(s) = \sum_{n=1}^{\infty} \frac{\Lambda_1(n)}{n^s} = \mathcal{P}(s) + \underbrace{\sum_{k\geqslant 2} \frac{\mathcal{P}(ks)}{k}}_{\text{beschr. für } s \geqslant 1} .$$

Verhalten für $s \searrow 1$:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \sim \frac{1}{s-1}, \quad \mathcal{P}(s) = \sum_{p} \frac{1}{p^s} \sim \log\frac{1}{s-1},$$

insbesondere $\displaystyle\sum_p \frac{1}{p} = \infty$ (Euler).

B. Möbiusscher Umkehrsatz; verschiedene Versionen und Anwendungen

Die Möbius-Funktion $\mu : \mathbb{N}_1 \to \mathbb{Z}$ ist definiert durch

$$\mu(n) := \begin{cases} 0, & \text{falls } n \text{ nicht quadratfrei,} \\ (-1)^r, & \text{falls } n \text{ quadratfrei und } r \text{ verschiedene Primteiler hat.} \end{cases}$$

Für $n \leqslant 14$ ergeben sich folgende Werte

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1	1

Ein erstes interessantes Auftreten der Möbiusfunktion ist die Dirichlet-Reihe von $1/\zeta(s)$

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

1) Der klassische Möbiussche Umkehrsatz lautet:
Sei $f : \mathbb{N}_1 \to \mathbb{C}$ eine arithmetischen Funktion. Die sog. summatorische Funktion von f ist definiert durch

$$F(n) := \sum_{k|n} f(k).$$

(Dabei wird über alle Teiler k von n summiert; z.B. $F(6) = f(1) + f(2) + f(3) + f(6)$.)
Dann kann man f aus F wieder zurückgewinnen durch

$$f(n) = \sum_{k|n} \mu(k) F\Big(\frac{n}{k}\Big) = \sum_{k|n} \mu\Big(\frac{n}{k}\Big) F(k) = \sum_{k\cdot\ell=n} \mu(k) F(\ell).$$

Es gibt viele Varianten des Umkehrsatzes, z.B.

2) Sei $f : [1, +\infty[\to \mathbb{C}$ eine beliebige komplexwertige Funktion und

$$F(x) := \sum_{k\leqslant x} f\Big(\frac{x}{k}\Big) \quad \text{für } x \geqslant 1.$$

Dabei wird über alle natürliche Zahlen $k \leqslant x$ summiert. Dann gilt

$$f(x) = \sum_{k\leqslant x} \mu(k) F\Big(\frac{x}{k}\Big).$$

3) Sei $f : [1, +\infty[\to \mathbb{C}$ eine Funktion mit $f(x) = 0$ für $x < 1 + \varepsilon$, $(\varepsilon > 0)$, und

$$F(x) := \sum_{k=1}^{\infty} f(x^{1/k}).$$

Dann folgt

$$f(x) = \sum_{k=1}^{\infty} \mu(k) F(x^{1/k}).$$

4) Sei $f : [1, +\infty[\to \mathbb{C}$ eine Funktion mit $f(x) = O(1/x^{\varepsilon})$ für $x \to \infty$ und

$$F(x) = \sum_{k=1}^{\infty} \frac{f(kx)}{k}$$

Dann folgt

$$f(x) = \sum_{k=1}^{\infty} \mu(k) \frac{F(kx)}{k}.$$

5) Sei $f : [1, +\infty[\to \mathbb{C}$ eine beliebige komplexwertige Funktion und $\alpha : \mathbb{N}_1 \to \mathbb{C}$ eine vollständig multiplikative Funktion.
Die Funktion $F : [1, +\infty[\to \mathbb{C}$ werde definiert durch

$$F(x) = \sum_{k \leqslant x} \alpha(k) f\Big(\frac{x}{k}\Big).$$

Dann folgt

$$f(x) = \sum_{k \leqslant x} \mu(k)\alpha(k) F\Big(\frac{x}{k}\Big).$$

6) Sei G eine abelsche multiplikativ geschriebene Gruppe und $f : \mathbb{N}_1 \to G$ eine beliebige Funktion. Sei

$$F(n) := \prod_{k|n} f(k).$$

Dann folgt

$$f(n) = \prod_{k|n} F(d)^{\mu(n/k)}$$

Eine Anwendung von 6) ist z.B.:
Sei $\Phi_n(X) \in \mathbb{Q}[X]$ das n-te Kreisteilungs-Polynom. Es gilt bekanntlich

$$X^n - 1 = \prod_{k|n} \Phi_k(X).$$

Es folgt

$$\Phi_n(X) = \prod_{k|n} (X^k - 1)^{\mu(n/k)}$$

Die Gruppe im Sinne von 6) ist hier $G = \mathbb{Q}(X) \setminus 0$, die multiplikative Gruppe des Funktionenkörpers $\mathbb{Q}(X)$ und $f(n) = X^n - 1$, $F(n) = \Phi_n(X)$.

Lit.: [Apo], Thm. 2.9 and Thm. 2.23,

Vorl. WiSe 2001/02, Chap. 3.

Vorl. SoSe 2008, Kap. 5

C. Euler-Mascheronische Konstante und Dirichletscher Teilersatz

Die Euler-Mascheronische Konstante ist definiert als

$$\gamma := \lim_{N\to\infty}\Big(\sum_{n=1}^{N}\frac{1}{n} - \log N\Big) = 0.57721\ldots$$

Es besteht ein bemerkenswerter Zusammenhang mit der Teilerfunktion $\tau(n)$. Nach Definition ist $\tau(n)$ die Anzahl der (positiven) Teiler einer natürlichen Zahl n (einschließlich der trivialen Teiler 1 und n). Z.B. gilt

$$\tau(1) = 1, \quad \tau(2) = 2, \quad \tau(3) = 2, \quad \tau(4) = 3, \ \ldots, \ \tau(12) = 6, \ \ldots$$

Dirichlet hat bewiesen: Für reelles $x \geqslant 1$ gilt

$$\sum_{n\leqslant x}\tau(n) = x(\log x + 2\gamma - 1) + O(\sqrt{x}).$$

Daraus folgt:

$$\lim_{x\to\infty}\frac{1}{x}\sum_{n\leqslant x}\tau(n) = \log x + (2\gamma - 1); \qquad 2\gamma - 1 = 0.154\ldots.$$

Die durchschnittliche Anzahl der Teiler einer natürlichen Zahl $n \leqslant x$ ist also asymptotisch gleich $\log x + (2\gamma - 1)$.

Im Vortrag soll die Existenz des Limes bei der Definition der Euler-Mascheronischen Konstante gezeigt und dann der Dirichletsche Teilersatz bewiesen werden, wobei insbesondere auf die Beweismethode, den sog. Hyperbeltrick, einzugehen ist.

Lit.: Vorl. WiSe 2008/09, Kap. 3.
[Apo], Chap. 3.5.

D. $\zeta(2)$ und die asymptotische Dichte der quadratfreien Zahlen und der Paare teilerfremder Zahlen

Euler hat bewiesen, dass

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} = 1.64493\ldots$$

1) Es gibt einen bemerkenswerten Zusammenhang dieser Zahl mit der Häufigkeit quadratfreier Zahlen, d.h. natürlicher Zahlen n, die durch kein Quadrat einer Primzahl teilbar sind. Die Liste der quadratfreien Zahlen beginnt mit

$$1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, \ldots$$

Für eine natürliche Zahl N bezeichnen wir mit $\mathrm{Sqfr}(N)$ die Menge aller quadratfreien natürlichen Zahlen $n \leqslant N$. (Sqfr von engl. *squarefree*) und mit $\#\mathrm{Sqfr}(N)$ deren Anzahl. Dann gilt

$$\lim_{N\to\infty} \frac{\#\mathrm{Sqfr}(N)}{N} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2} = 0.6079\ldots$$

Man kann dies so interpretieren, dass durchschnittlich etwa 61 Prozent der natürlichen Zahlen quadratfrei sind.

2) Analog gibt es eine Aussage über die Wahrscheinlichkeit, dass zwei unabhängig zufällig gewählte natürliche Zahlen n, k teilerfremd sind. Wir bezeichnen mit $\mathrm{Copr}(N)$ die Menge aller Paare n, k natürlicher Zahlen mit $n, k \leqslant N$ und $\gcd(n, k) = 1$. (Copr von engl. *coprime* = teilerfremd.)
Hier gilt

$$\lim_{N\to\infty} \frac{\#\mathrm{Copr}(N)}{N^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

In dem Vortrag sollen die Formel $\zeta(2) = \pi^2/6$ und die Aussagen 1) und 2) bewiesen werden.

Lit.: [Fo2] für $\zeta(2)$,
Vorl. WiSe 2001/02, Chap. 4, Thm. 4.10, für $\mathrm{Copr}(N)$

DZ. Elementare Abschätzungen zur Primzahlverteilung, Bertrandsches Postulat

Für eine reelle Zahl $x > 1$ bezeichne $\pi(x)$ die Anzahl der Primzahlen $\leqslant x$. Schon Legendre und Gauß haben vermutet, dass $\pi(x)$ asymptotisch gleich $\dfrac{x}{\log x}$ ist, d.h.

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

Diese Aussage, der sog. Primzahlsatz, wurde 1896 unabhängig von J. Hadamard und Ch. de la Vallée Poussin bewiesen.

In diesem Seminar soll mit elementaren Mitteln nur eine abgeschwächte Aussage, nämlich

$$\frac{1}{2} \cdot \frac{x}{\log x} \leqslant \pi(x) \leqslant 4 \cdot \frac{x}{\log x}, \quad (x \geqslant 3), \tag{$*$}$$

bewiesen werden. Eine wichtige Rolle spielen dabei die von Tschebyscheff eingeführten Funktionen

$$\vartheta(x) := \sum_{p\leqslant x} \log p,$$
$$\psi(x) := \sum_{p^k\leqslant x} \log p.$$

Der Primzahlsatz ist äquivalent zu den asymptotischen Beziehungen $\vartheta(x) \sim x$ und $\psi(x) \sim x$ für $x \to \infty$. Im Seminar sollen nur Abschwächungen davon bewiesen werden, aus denen man $(*)$ folgern kann.

Eine weitere Aussage, die man damit beweisen kann, ist das sog. Bertrandsche Postulat, das besagt, dass zu jedem $n \in \mathbb{N}_1$ eine Primzahl p existiert mit

$$n < p \leqslant 2n.$$

Lit. Skript PZV_Bertrand.pdf

E. Fermatsche und Mersennesche Primzahlen

a) Eine Zahl der Gestalt 2^n+1 ist höchstens dann prim, wenn $n = 2^k$ eine Zweierpotenz ist. Fermat glaubte, dass alle Zahlen der Gestalt $F_k := 2^{2^k} + 1$, $k = 0, 1, 2, 3, \ldots$ Primzahlen seien. Dies ist zwar richtig für $k = 0, 1, 2, 3, 4$, aber schon $F_5 = 4294967297 = 641 \cdot 6700417$ ist eine zusammengesetzte Zahl. Bisher wurden keine weiteren Fermatschen Primzahlen gefunden. Von Pépin stammt folgendes Kriterium:

$F_k = 2^{2^k} + 1$ ist genau dann prim, wenn $3^{(F_k-1)/2} \equiv -1 \bmod F_k$

Ist F_k nicht prim, so haben die Primteiler p von F_k eine spezielle Gestalt: Es ist $p = h \cdot 2^{k+2} + 1$ mit einer ganzen Zahl $h \geqslant 1$. Z.B. ist der oben genannte Teiler von F_5 gleich $p = 5 \cdot 2^7 + 1$.

b) Eine Zahl der Gestalt $2^n - 1$ ist höchstens dann prim, wenn der Exponent n eine Primzahl ist. Aber nicht für jede Primzahl p ist die sog. Mersenne-Zahl $M_p = 2^p - 1$ prim. Es gilt das folgende Kriterium von Lucas:

Sei $n \geqslant 3$ ungerade. Genau dann ist $M_n = 2^n - 1$ eine Primzahl, wenn für die wie folgt rekursiv definierte Folge (v_k) ganzer Zahlen

$$\begin{aligned} v_0 &:= 4, \\ v_k &:= v_{k-1}^2 - 2, \quad (k \geqslant 1), \end{aligned}$$

gilt: $v_{n-2} \equiv 0 \bmod M_n$.

Ist M_p nicht prim, so haben die Primteiler q von M_p eine spezielle Gestalt: Es ist $q = 2kp + 1$ mit einer ganzen Zahl k. Außerdem gilt $q = \pm 1 \bmod 8$.
Z.B. ist $M_{11} := 2^{11} - 1 = 2047 = 23 \cdot 89$ und

$$\begin{aligned} 23 &= 2 \cdot 11 + 1, \qquad 23 \equiv -1 \bmod 8, \\ 89 &= 8 \cdot 11 + 1, \qquad 89 \equiv +1 \bmod 8. \end{aligned}$$

Im Vortrag sollen diese Aussagen bewiesen werden.

Lit.: [Fo1], Sätze 11.5 und 11.6, [MSP] Sätze 11.1 und 11.3

F. Periodische Dezimalbrüche und der Satz von Midy

Ist p eine Primzahl $\neq 2, 5$, so ist die Periodenlänge des Dezimalbruchs a/p, $(0 < a < p)$ höchstens gleich $p-1$, und in jedem Fall ein Teiler von $p-1$. Ein Fall, in dem die maximale Periodenlänge eintritt, ist $p = 7$. Man beobachtet folgende interessante Erscheinungen:

$$
\begin{aligned}
1/p &= 0.\overline{142857},\\
3/p &= 0.\overline{428571},\\
2/p &= 0.\overline{285714},\\
6/7 &= 0.\overline{857142},\\
4/7 &= 0.\overline{571428},\\
5/7 &= 0.\overline{714285}.
\end{aligned}
$$

Die Ziffern der Periode 142857 werden also zyklisch vertauscht.

Eine analoge Erscheinung erhält man für $p = 17$, wo die Periodenlänge 16 beträgt.

$$1/17 = 0.\overline{0588235294117647}$$

Dahinter steht die Tatsache, dass die Periodenlänge genau dann gleich $p-1$ ist, falls $(10 \bmod p)$ eine Primitivwurzel modulo p ist.

Für $p = 13$ ist dies nicht der Fall, hier hat 10 in der mulitplikativen Gruppe $(\mathbb{Z}/13)^*$ die Ordnung 6, dies ist gleichzeitig die Periodenlänge; es ist

$$1/13 = 0.\overline{076923}$$

In allen drei Fällen gilt jedoch: Teilt man die Periode in der Mitte (falls die Periodenlänge gerade ist) und addiert diese Zahlen, so erhält man

$$
\begin{array}{rrr}
142 & 05882352 & 076\\
+857 & +94117647 & +923\\
\hline
999 & 99999999 & 999
\end{array}
$$

Dies sind Beispiele für den Satz von Midy.

Im Vortrag sollen die angesprochenen Aussagen über die Perioden und der Satz von Midy bewiesen werden und auch auf andere Basen als 10 verallgemeinert werden.

Lit.: [KW] Abschnitt 7.3.1

G. Summen von 2 und 4 Quadraten

1) Nach Fermat ist eine ungerade Primzahl p genau dann eine Summe von 2 Quadratzahlen, wenn $p \equiv 1 \bmod 4$. Aufgrund der Multiplikativität der Normfunktion im Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen folgt daraus: Eine natürliche Zahl n ist genau dann Summe von zwei Quadraten, wenn in der Primfaktorzerlegung von n die Primfaktoren $p \equiv 3 \bmod 4$ mit gerader Vielfachheit auftreten.

2) Ein Satz von Lagrange besagt, dass sich jede natürliche Zahl als Summe von 4 Quadratzahlen darstellen lässt. Aufgrund der Multiplikativität der Normfunktion im Ring $\mathbb{H}_{\mathbb{Z}}$ der ganzzahlige Quaternionen braucht man das nur für Primzahlen p beweisen.

Die sog. *Abstiegsmethode* zum Beweis besteht darin, dass man sich zunächst eine Darstellung

$$\sum_{\nu=1}^{4} x_\nu^2 = kp, \quad k \in \mathbb{N}_1$$

beschafft und daraus analoge Darstellungen mit kleinerem k konstruiert, bis man bei $k = 1$ angelangt ist.

Eine andere Beweismethode benutzt die Geometrie der Zahlen (Minkowskischer Gitterpunktsatz)

Im Seminar sollen beide Methoden dargestellt werden.

Lit.: [SO], Kap. 9, [MSP], Satz 9.2 und Satz 9.6, [KW] Satz 11.3,
Skript sum24Q.pdf

H. Charaktere endlicher abelscher Gruppen und Dirichletsche L-Reihen

Sei G eine multiplikativ geschriebene endliche abelsche Gruppe der Ordnung $r := \#G$. Unter einem Charakter von G versteht man einen Gruppen-Homomorphismus

$$\chi : G \longrightarrow \mathbb{C}^*.$$

Die Menge aller Charaktere wird mit $\widehat{G}$ bezeichnet. Auf $\widehat{G}$ hat man eine natürliche Verknüpfung, mit der $\widehat{G}$ wieder eine abelsche Gruppe wird, die ebenso viele Elemente wie G besitzt. Es gelten die Orthogonalitäts-Relationen ($x, y \in G$, $\chi, \psi \in \widehat{G}$)

$$\sum_{x \in G} \overline{\chi(x)}\psi(x) = \begin{cases} r, & \text{falls } \chi = \psi, \\ 0, & \text{falls } \chi \neq \psi. \end{cases}$$

$$\sum_{\chi \in \widehat{G}} \overline{\chi(x)}\chi(y) = \begin{cases} r, & \text{falls } x = y, \\ 0, & \text{falls } x \neq y. \end{cases}$$

Die wichtigste Anwendung ist die multiplikative Restklassen-Gruppe $G := (\mathbb{Z}/m)^*$, ($m \geqslant 2$). Hier gilt $\#(\mathbb{Z}/m)^* = \varphi(m)$, (Eulersche Phi-Funktion).

Ein Dirichlet-Charakter modulo m ist eine Abbildung

$$\chi : \mathbb{Z} \longrightarrow \mathbb{C},$$

für die es einen Charakter $\widetilde{\chi} \in \widehat{(\mathbb{Z}/m)^*}$ gibt, so dass

$$\chi(x) = \begin{cases} \widetilde{\chi}(x \bmod m), & \text{falls } \gcd(x, m) = 1, \\ 0, & \text{falls } \gcd(x, m) > 1. \end{cases}$$

Der sog. Hauptcharakter $\chi_{0m} : \mathbb{Z} \longrightarrow \mathbb{C}$ entspricht dem Einheits-Charakter der Gruppe $(\mathbb{Z}/m)^*$, d.h.

$$\chi_{0m}(x) = \begin{cases} 1, & \text{falls } \gcd(x, m) = 1, \\ 0, & \text{falls } \gcd(x, m) > 1 \end{cases}$$

Jedem Dirichlet-Charakter modulo m ist eine sog. Dirichletsche L-Reihe zugeordnet:

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Es gilt: Ist χ nicht der Hauptcharakter, so konvergiert die Reihe $L(s, \chi)$ für alle $s > 0$. Dies liegt daran, dass

$$\sum_{n \leqslant x} \chi(n) = O(1) \quad \text{für } x \to \infty.$$

Es gilt nämlich der

Satz. *Sei $a : \mathbb{N}_1 \to \mathbb{C}$ eine arithmetische Funktion mit beschränkten Partialsummen, d.h.*

$$\sum_{n \leqslant x} a(n) = O(1) \quad \textit{für } x \to \infty.$$

Dann konvergiert die Dirichlet-Reihe

$$f(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

für alle $s > 0$.

Für den Hauptcharakter hat man

$$L(s, \chi_{0m}) = \sum_{\substack{n \geqslant 1 \\ \gcd(n,m)=1}} \frac{1}{n^s} = \prod_{p|m} \Big(1 - \frac{1}{p^s}\Big) \zeta(s)$$

Für diese Funktion gilt daher

$$\lim_{s \searrow 1} L(s, \chi_{0m}) = \infty,$$

genauer

$$\lim_{s \searrow 1} (s-1) L(s, \chi_{0m}) = \frac{\varphi(m)}{m}.$$

Lit. Skript charLseries.pdf

I. Nichtverschwinden von $L(1,\chi)$ für Nicht-Hauptcharaktere χ

Ist $\chi : \mathbb{Z} \to \mathbb{C}$ ein Dirichlet-Charakter modulo m, der vom Hauptcharakter χ_{0m} verschieden ist, so konvergiert die L-Reihe $L(s,\chi)$ für alle $s > 0$, also ist der Wert $L(1,\chi) \in \mathbb{C}$ definiert. Die Tatsache, dass $L(1,\chi) \neq 0$, ist ganz wesentlich beim Beweis des Dirichletschen Satzes über Primzahlen in arithmetischen Progressionen.

Zum Beweis versucht man die Annahme $L(1,\chi) = 0$ zum Widerspruch zu führen. Dabei spielt es eine große Rolle, ob χ ein reeller Charakter ist, d.h. nur reelle Werte annimmt, oder ein sog. komplexer Charakter, der auch nicht-reelle Werte annimmt. Der letztere Fall ist der einfachere, denn dann gilt auch für den konjugierten Charakter $\overline{\chi}$, dass $L(1,\overline{\chi}) = 0$. Für das Produkt

$$\Phi_m(s) = \prod_{\chi} L(s,\chi),$$

wobei das Produkt über alle Charaktere modulo m gebildet wird (einschließlich des Hauptcharakters), kann man zeigen

$$\liminf_{s \searrow 1} \Phi_m(s) \geqslant 1.$$

Falls aber zwei Faktoren $L(s,\chi)$ und $L(s,\overline{\chi})$ bei $s = 1$ eine Nullstelle haben, überwiegt dies den Pol von $L(s,\chi_{0m})$ an der Stelle $s = 1$ und es würde folgen $\lim_{s \searrow 1} \Phi_m(s) = 0$, Widerspruch!

Dieser Beweis versagt im Fall eines reellen Charakters. In diesem Fall gibt es einen Beweis, der auf der genaueren Untersuchung des Produkts

$$f(s) := \zeta(s) L(s,\chi)$$

beruht. Dabei zeigt man, dass unter der Voraussetzung $L(1,\chi) = 0$ die Partialsummen der Dirichlet-Reihe von $f(s)$ an der Stelle $s = \frac{1}{2}$ beschränkt bleiben und führt dies zu einem Widerspruch.

Es gibt noch viele andere Beweismethoden für $L(1,\chi) \neq 0$.

Lit.: [Apo], Thm. 6.20, [Mo]

J. Dirichletscher Satz über Primzahlen in arithmetischen Progressionen

Die Primzahlen $p \neq 2$ zerfallen in zwei Klassen:
Erstens die Primzahlen $p \equiv 1 \bmod 4$,

$$5, 13, 17, 29, 37, 41, \ldots.$$

und zweitens die Primzahlen $p \equiv 3 \bmod 4$,

$$3, 7, 11, 19, 23, 31, 43, \ldots.$$

Jede dieser Klassen enthält unendlich viele Primzahlen.
Dies lässt sich im Fall $p \equiv 3 \bmod 4$ analog zum Euklidischen Beweis für die Unendlichkeit der Primzahlen zeigen: Angenommen, es gebe nur endlich viele Primzahlen $q_\nu \equiv 3 \bmod 4$, $\nu = 1, \ldots, r$. Man bilde das Produkt

$$Q_3 := 4q_1 \cdot q_2 \cdot \ldots \cdot q_r - 1.$$

Es gilt $Q_3 \equiv 3 \bmod 4$. Dann muss Q_3 durch mindestens eine Primzahl $q \equiv 3 \bmod 4$ teilbar sein (der Fall $q = Q_3$ ist auch möglich), denn ein Produkt von lauter Primzahlen $\equiv 1 \bmod 4$ ist wieder $\equiv 1 \bmod 4$. Außerdem ist q von allen q_ν verschieden. Also waren $q_1, \ldots, q_r$ nicht alle Primzahlen $\equiv 3 \bmod 4$, Widerspruch!

Ein entsprechender Beweisansatz für Primzahlen $p \equiv 1 \bmod 4$ scheitert. Denn sei

$$Q_1 := 4p_1 \cdot p_2 \cdot \ldots \cdot p_s + 1.$$

Dann ist zwar $Q_1 \equiv 1 \bmod 4$, aber Q_1 könnte nur aus Primzahlen $p \equiv 3 \bmod 4$ zusammengesetzt sein, Beispiel

$$4 \cdot (5 \cdot 13 \cdot 17 \cdot 29 \cdot 37) + 1 = 4742661 = 3 \cdot 7 \cdot 7 \cdot 7 \cdot 11 \cdot 419.$$

Unter Benutzung des 1. Ergänzungssatzes des quadratischen Reziprozitätsgesetzes gelingt aber der Beweis: Sei

$$P_1 := 4\,(p_1 \cdot p_2 \cdot \ldots \cdot p_s)^2 + 1.$$

Dafür gilt: Jeder Primteiler $p \mid P_1$ ist von allen q_ν verschieden. Da $P_1 \equiv 0 \bmod p$, folgt

$$(2\,p_1 \cdot p_2 \cdot \ldots \cdot p_s)^2 \equiv -1 \bmod p,$$

d.h. -1 ist ein Quadrat modulo p. Das bedeutet aber

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = 1 \quad \Longrightarrow \quad p \equiv 1 \bmod 4.$$

Der allgemeine Satz von Dirichlet über Primzahlen in arithmetischen Progressionen lautet:
Sei $m \geqslant 2$ und a eine ganze Zahl mit $0 < a < m$ und $\gcd(a, m) = 1$. Dann gibt es unendlich viele Primzahlen $p \equiv a \bmod m$. In einem gewissen Sinn gibt es sogar asymptotisch gleichviele Primzahlen in allen $\varphi(m)$ teilerfremden Restklassen a mod m. Dies lässt sich so präzisieren: Für reelles $x > 0$ sei

$$P(x) := \sum_{p \leqslant x} \frac{1}{p}.$$

Dabei wird über alle Primzahlen $p \leqslant x$ summiert. Nach Euler gilt $\lim_{x\to\infty} P(x) = \infty$. Analog sei für $\gcd(a, m) = 1$

$$P_{a,m}(x) := \sum_{\substack{p \leqslant x \\ p \equiv a \bmod p}} \frac{1}{p}.$$

Dabei wird nur über alle Primzahlen $p \leqslant x$ mit $p \equiv a \bmod m$ summiert. Damit gilt dann

$$(\diamond) \quad \lim_{x\to\infty} \frac{P_{a,m}(x)}{P(x)} = \frac{1}{\varphi(m)}.$$

Zum Beweis benutzt Dirichlet die Theorie der Charaktere modulo m. Für $\chi \in \widehat{(\mathbb{Z}/m)^*}$ und $x > 0$ sei

$$P(x, \chi) := \sum_{p \leqslant x} \frac{\chi(p)}{p}.$$

Für den Hauptcharakter χ_{0m} gilt

$$P(x, \chi_{0m}) = \sum_{p \leqslant x,\, p \nmid m} \frac{1}{p}.$$

Ein wesentlicher Punkt ist, dass für einen Nicht-Hauptcharakter χ die Summen $P(x, \chi)$ für $x \to \infty$ beschränkt bleiben; sogar der Limes

$$\lim_{x\to\infty} P(x, \chi) = \sum_{p} \frac{\chi(p)}{p} \qquad \text{(Summation über alle Primzahlen } p\text{)}$$

existiert. Aufgrund der Orthogonalitäts-Relationen für Dirichlet-Charaktere gilt

$$\begin{aligned} \varphi(m) P_{a,m}(x) &= \sum_{\chi} \overline{\chi}(a) P(x, \chi) \\ &= P(x, \chi_{0m}) + \sum_{\chi \neq \chi_{0,m}} \overline{\chi}(a) P(x, \chi). \end{aligned}$$

Dividiert man durch $P(x)$ und geht zum Limes $x \to \infty$ über, erhält man die Behauptung $(\diamond)$

K. Die Legendre-Gleichung

Die Legendre-Gleichung lautet

$$ax^2 + by^2 + cz^2 = 0.$$

Dabei sind a, b, c vorgegebene, von Null verschiedene ganze Zahlen. Gesucht ist eine ganzzahlige Lösung $(x, y, z) \neq (0, 0, 0)$. O.B.d.A. ist $\gcd(a, b, c) = 1$. Außerdem kann der allgemeine Fall leicht auf den Fall zurüchgeführt werden, dass die Koeffizienten quadratfrei sind.

Für den Beweis des Drei-Quadrate-Satzes brauchen wir nur folgenden Spezialfall.

Satz. *Seien $a, b \in \mathbb{Z} \setminus \{0\}$ quadratfreie, teilerfremde ganze Zahlen, die nicht beide negativ sind. Genau dann besitzt die Gleichung*

$$ax^2 + by^2 = z^2$$

eine Lösung $(x, y, z) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$, wenn folgende Bedingungen erfüllt sind:

(i) *a ist ein Quadrat modulo b,*

(ii) *b ist ein Quadrat modulo a.*

Falls $\gcd(a, b) = d > 1$, so ist folgende zusätzliche Bedingung zu stellen:

Setze $a_1 := a/d$ und $b_1 := b/d$. Damit lautet die Zusatzbedingung:

(iii) *$-a_1 b_1$ ist ein Quadrat modulo d.*

Lit.: Skript LegSum3Q.pdf und [Dav], Chap. VII, 3.

L. Summen von 3 Quadraten

Nicht jede natürliche Zahl ist die Summen von drei Quadratzahlen, z.B. lässt sich die Zahl 7 nicht in der Form $7 = x^2 + y^2 + z^3$ mit $x, y, z \in \mathbb{Z}$ darstellen, wovon man sich leicht direkt überzeugen kann. Die allgemeine Aussage wird durch folgenden Satz wiedergegeben:

Satz. *Eine natürliche Zahl n ist genau dann Summe von 3 Quadraten, d.h.*

$$n = x^2 + y^2 + z^2 \quad \textit{mit } x, y, z \in \mathbb{Z},$$

wenn $n = 4^k m$ mit $4 \nmid m$ und $m \not\equiv 7 \bmod 8$.

Der allgemeine Fall kann leicht auf den Fall $k = 0$ zurückgeführt werden.

Zum Beweis benutzt man einen Satz von L. Aubry, dass es genügt, n als Summe von drei Quadraten rationaler Zahlen darzustellen, oder, was nach Multiplikation mit dem Hauptnenner auf dasselbe hinausläuft, $(t, x, y, z) \in \mathbb{Z}^4$ mit $t \neq 0$ zu finden, so dass

$$nt^2 = x^2 + y^2 + z^2.$$

Dann konstruiert man mithilfe des Dirichletschen Primzahlsatzes im Fall $n \equiv 1 \bmod 4$ oder $n \equiv 2 \bmod 4$ eine Primzahl $p \equiv 1 \bmod 4$, so dass die Legendre-Gleichung

$$nt^2 - py^2 = z^2$$

lösbar ist. Nun ist nach Fermat p eine Summe von 2 Quadraten, $p = u^2 + v^2$. Setzt man dies ein, so erhält man

$$nt^2 = (uy)^2 + (vy)^2 + z^2,$$

also nach Aubry auch eine Darstellung von n als Summe von 3 Qudaratzahlen.

Im noch ausstehenden Fall $n \equiv 3 \bmod 8$ findet man eine Primzahl $p \equiv 1 \bmod 4$, so das die Legendre-Gleichung

$$nt^2 - 2py^2 = z^2$$

lösbar ist, und man schließt ähnlich.

Aus dem 3-Quadrate-Satz folgt, dass jede natürliche Zahl eine Summe von 3 Dreieckszahlen ist, d.h. von 3 Zahlen der Gestalt $\Delta_\nu = \dfrac{\nu(\nu+1)}{2}$.

Lit.: Skript LegSum3Q.pdf

Literatur

[Apo] T. Apostol: Introduction to Analytic Number Theory. Springer

[Dav] H. Davenport: The Higher Arithmetic. Cambridge U.P.

[Fo1] O. Forster: Algorithmische Zahlentheorie. 2.Aufl. Springer

[Fo2] O. Forster: Analysis 1. 12.Aufl. Springer Spektrum

[KW] Kraft/Washington: An Introduction to Number Theory with Cryptography. CRC Press.

[Mo] P. Monski: Simplifying the Proof of Dirichlet's Theorem. Amer. Math. Montly **100** (1993) 861 – 862.

[MSP] Müller-Stach/Piontkowski: Elementare und algebraische Zahlentheorie. 2.Aufl. Vieweg 2011

[SO] Scharlau/Opolka: Von Fermat bis Minkowski. Springer